ABSTRACT OF THE DISCLOSURE

Registration of non-configured network devices in a distributed network is facilitated by a method of distributing cryptographic keys. A non-configured first device seeking to communicate securely with a second device acquires knowledge of a trusted registration service. The first device registers with the registration service and obtains a longer-lived symmetric key. Using the longer-lived key, the first device authenticates itself to a key management service, and receives a shorter-lived symmetric key encapsulated in a ticket that includes policy information. A second device carries out the same preparatory process. Using its ticket containing the shorter-lived key, the first device requests the second device to obtain a session key on behalf of both. The second device presents its own ticket and that of the first device to the key management service to authenticate the shorter-lived key, and then obtains a session key for use in communications among the first and second devices. The first device and second device then communicate by encrypting communications with the session key, and without further contact with the key management or registration services or any other online authoritative server or key database. Thus newly deployed network devices may be positively identified, registered in the network, and subjected to key schedule or other key management policies.